REMARKS

Claims 1-20 are pending. Claims 1-20 are rejected.

Claims 1-7, 10, 12, 16 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fan et al. (U.S. Patent No. 6,219,706) ("Fan"), in view of Coates et al. (U.S. Patent No. 7,203,731) ("Coates"). Claims 8-9 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fan, in view of Coates, in view of Lango (U.S. Patent No. 6,81,690) ("Lango"). Claims 11, 15 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fan, in view of Coates, further in view of Lewin (U.S. Patent No. 7,010,578) ("Lewin"). Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fan, in view of Coates, and in view of Lewin, further in view of Lango. Applicants respectfully traverse these rejections.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." MPEP 2143.03 (emphasis added). The combined references fail to teach or suggest all the claim limitations.

For example, Fan and Coates fail to teach or suggest "inspecting the payload section of the packet in a network core for use in determining how to route the packet to subscribers," as recited in claim 1, and similarly recited in independent claims 12 and 19.. Fan teaches access control for networks, not routing (indeed, Fan uses a router as a firewall for access control, not routing). The Office Action cites to col. 2, lines 28-35 and col. 4, lines 45-55 as purportedly teaching this. However, an examination of col. 2, lines 28-35 merely reveals Fan discussing, in its Background of the Invention, inspecting a packet payload for identifying channels in which port numbers are set by communicating nodes. Fan describes that by identifying the port numbers, the firewall can open a temporary channel corresponding to the port number. As is clear to one of ordinary skill in the art, this merely describes a standard, well-known firewall activity: opening a temporary channel permits the packet to pass through the firewall, *i.e.*, permitting access to the network or computer the firewall is protecting. Opening a temporary channel to permit access is not routing and does not route a packet and this section of Fan does not describe inspecting a payload section of a packet for use in determining how to route the packet. Indeed, the description at col. 4, lines 45-55 merely describes a router acting as a firewall and permitting a conversation from a node to a host, not routing a packet or determining how to route a packet to subscribers. Nowhere beyond the cited sections does Fan teach or suggest inspecting the payload section of the packet in a network core for use in determining how to route the packet to subscribers. Therefore, Fan does not describe inspecting the payload section of the packet in a network core for use in determining how to route the packet to subscribers. Coates does not cure this defect. Consequently, independent claims 1, 12 and 19 are not rendered obvious by Fan and Coates.

This point is further emphasized by showing that Fan and Coates fail to teach or suggest "selectively routing the packet based upon the inspecting," as recited in claims 1, 12 and 19. The Office Action cites to col. 8, lines 49-59 as purportedly teaching this feature. However, an examination of this cited section reveals that it is describing filtering packets based on an *inspection of the packet header*! The preceding paragraph in Fan, col. 8, lines 38-48 states"

> Various combinations of matching (or not matching) *packet header fields* can be used to support a policy. Examples of specific fields that may be examined include IP destination address, IP source address, IP protocol field, TCP source port, TCP destination port...All or some of that information may be compared ...and/or used by the firewall engine to determine whether the packet is appropriate given the current state of the session.

(emphasis added). The cited col. 8, lines 49-59 then go on to state:

> In a specific example, an access control list item may specify the addresses of the communicating hosts...More specifically, for example, if the security access policy prevents SMTP sessions initiated from IP host 1.1.1.1. with a destination address 2.2.2.2 then the *packet filter would discard packets* that have IP destination address=2.2.2.2., IP source address=1.1.1.1., IP protocol=6 (for TCP) and Destination port=25 (for SMTP). Such criteria may represent static Access Control List items.

(emphasis added). As stated, Fan is describing inspecting the packet header, not the packet payload, and filtering packets based on information in the packet header (*e.g.*, the IP destination address, IP source address, IP protocol field, TCP source port, TCP destination port). Moreover, Fan is not even routing based on the packet header information, but merely filtering out as part of access control. No other portion of Fan describes selectively routing based on a payload inspection. Therefore, Fan does not describe selectively routing the packet based upon the inspecting. Coates does not cure this defect. Consequently, independent claims 1, 12 and 19 are not rendered obvious by Fan and Coates.

The additional cited references, Lango and Lewin do not cure these defects. Consequently, dependent claims 2-11, 13, 15-18 and 20 are also not rendered obvious for at least the above reasons and their own independent features. Allowance of claims 1-13 and 15-20 is respectfully requested.

CONCLUSION

Applicants respectfully submit that the application is in condition for allowance. Therefore, Applicants respectfully request that a timely Notice of Allowance be issued in this application.

If the Examiner believes that a personal or telephonic interview would be of value in expediting the prosecution of this application, the Examiner is hereby invited to telephone the undersigned counsel to arrange for such a conference.

Respectfully submitted,

Date: November 20, 2008

Sean Wooden
Reg. No. 43,997
ANDREWS KURTH LLP
1350 I Street, N.W.
Suite 1100
Washington, D.C. 20005
Telephone: (202) 662-2700
Fax: (202) 662-2739